

## REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application in light of the changes above and the remarks that follow. Claims 34-37 are pending in the application. By this Amendment, Applicant has amended claims 24, 27, 31 and 34 to clarify the recited subject matter. Support for the changes to claims 24 and 31 may be found in Applicant's specification at, for example, page 12, lines 5-12.

In the Final Office Action, the Examiner rejected claim 24 under 35 U.S.C. § 103(a) as allegedly not being patentable over U.S. Patent No. 6,278,783 ("Kocher1") in view of U.S. Patent No. 6,327,661 to ("Kocher2").<sup>1</sup> Present claim 24 recites, *inter alia*, a "DES cryptographic algorithm in which multiple rounds of calculation are performed on input data, said DES cryptographic algorithm being divided into stages including a plurality of successive rounds ... wherein, for some, but less than all, of said stages of said DES cryptographic algorithm, at least one of said first and second permutations of data comprises the following ...." Applicant traverses the rejection under Section 103(a) because the purported combination of Kocher1 and Kocher2 fails to disclose or suggest at least these features of claim 24.

In particular, neither Kocher1 nor Kocher2 disclose anything with regard to a "DES cryptographic algorithm being divided into stages including a plurality of successive rounds" or that "some, but less than all, of said stages" perform the claimed "selecting a first random value," "performing an exclusive-OR operation between the data being permuted and the first random value," "executing said permutation operation" and "performing an exclusive-OR operation between said first and second random results" (emphasis added). Accordingly, when Kocher1 and Kocher2 are taken individually or in combination, the patents cannot support a rejection of claim 24 under Section 103. Applicant, therefore,

---

<sup>1</sup> The Office Action contains statements characterizing the claims and related art. Regardless of whether any such statements are specifically addressed herein, Applicant's silence as to these characterizations should not be construed as acceptance of them.

requests reconsideration and allowance of claim 24, as well as claims 25-30, which are also allowable at least due to their dependence from claim 24.

Claim 31, although of different scope than claim 24, recites subject matter similar to that recited in claim 24. Thus, claim 31 is allowable over Kocher<sup>1</sup> and Kocher<sup>2</sup> for the same reason given above for claim 24. Claims 32-37 are allowable at least due to their dependence from claim 31.

For the reasons set forth above, Applicant respectfully requests that prosecution of this Application be reopened and that the pending claims be allowed.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: June 12, 2008

By: /Steven Ashburn/  
Steven L. Ashburn  
Registration No. 56,636

P.O. Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620